

Message Encoding for Spread and Orbit Codes

Anna-Lena Trautmann

Department of Electrical and Computer Systems Engineering
Monash University, Clayton, Australia

Department of Electrical and Electronic Engineering
University of Melbourne, Australia

Email: anna-lena.trautmann@unimelb.edu.au

Abstract—Spread codes and orbit codes are special families of constant dimension subspace codes. These codes have been well-studied for their error correction capability and transmission rate, but the question of how to encode messages has not been investigated. In this work we show how the message space can be chosen for a given code and how message en- and decoding can be done.

I. INTRODUCTION

Subspace codes are defined to be sets of subspaces of some given ambient space \mathbb{F}_q^n of dimension n over the finite field with q elements. When we talk about *constant dimension codes*, we restrict ourselves to subspace codes, whose codewords all have the same constant dimension. Subspace codes in general, and constant dimension codes in particular, have received much attention since it was shown in [11] how these codes can be used for random network coding.

In that same paper [11] a class of Reed-Solomon-like codes is proposed, which was shown to be equivalent to the lifting of maximum rank distance codes [18]. For these codes one can easily find a suitable message space (or message set) \mathcal{M} and an encoding map, that maps \mathcal{M} injectively to the subspace code.

During the last years other constructions of subspace codes were developed, e.g. in [1], [2], [3], [4], [6], [7], [10], [12], [19], [24]. Some of these constructions have the mere purpose of giving an improved transmission rate (i.e. larger cardinality of the code for the same parameters), while others also have some structure that can be used e.g. for decoding. The problem of message encoding has been addressed in almost none of these papers and is hence an open question for most of these codes. We want to study this problem for two classes of subspace codes, namely spread codes and orbit codes.

The paper is organized as follows: In the following section we will give some preliminaries, among others the spread code and orbit code construction. In Section III we investigate a natural message space and encoding map for Desarguesian spread codes, which we then extend to an encoding map on a set of integer numbers. In Section IV we do the same for orbit codes. In Section V we propose a hybrid encoding method, combining two encoding and decoding algorithms for spread codes. We conclude this work in Section VI.

The author was supported by Swiss National Science Foundation Fellowship No. 147304.

II. PRELIMINARIES

We denote the finite field with q elements by \mathbb{F}_q . The set of all subspaces of \mathbb{F}_q^n is denoted by $\mathcal{P}_q(n)$ and the set of all subspaces of \mathbb{F}_q^n of dimension k , called the *Grassmannian*, is denoted by $\mathcal{G}_q(k, n)$. We represent a vector space $\mathcal{U} \in \mathcal{G}_q(k, n)$ by a matrix $U \in \mathbb{F}_q^{k \times n}$ such that the row space of U , denoted by $\text{rs}(U)$, is equal to \mathcal{U} . A subspace code is simply a subset of $\mathcal{P}_q(n)$ and a constant dimension code is a subset of $\mathcal{G}_q(k, n)$. A metric on $\mathcal{P}_q(n)$ is given by the subspace distance ([11])

$$d_S(\mathcal{U}, \mathcal{V}) := \dim(\mathcal{U}) + \dim(\mathcal{V}) - 2\dim(\mathcal{U} \cap \mathcal{V})$$

for any $\mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n)$. The minimum distance $d_S(\mathcal{C})$ of a subspace code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is the minimum of all the pairwise distances of the codewords. Since the dual of a subspace code \mathcal{C} has the same minimum distance as \mathcal{C} (see e.g. [11]), it is customary to restrict oneself to $k \leq n/2$, which we will assume throughout the paper.

A *spread code* [12] in $\mathcal{G}_q(k, n)$ is defined as a set of elements of $\mathcal{G}_q(k, n)$ that pairwise intersect only trivially and cover the whole space \mathbb{F}_q^n . They exist if and only if $k|n$, have minimum distance $2k$ and cardinality $(q^n - 1)/(q^k - 1)$. For more information on different constructions and decoding algorithms of spread codes see [8], [12], [13], [20]. We will use the following construction, which gives rise to a *Desarguesian spread code* in $\mathcal{G}_q(k, n)$ ([20]):

- 1) Let $m := n/k$ and consider $\mathcal{G}_{q^k}(1, m)$, which has $q^{k(m-1)} + q^{k(m-2)} + \dots + 1 = (q^n - 1)/(q^k - 1)$ elements. Trivially, all these lines intersect only trivially.
- 2) Let P be the companion matrix of an irreducible polynomial over \mathbb{F}_q of degree k . Then it holds that $\mathbb{F}_{q^k} \cong \mathbb{F}_q[P]$ and we can use this isomorphism in any element of $\mathcal{G}_{q^k}(1, m)$ (i.e. we replace any coordinate with the respective matrix) to receive a spread code in $\mathcal{G}_q(k, n)$.

Example 1. Let α be a root of $x^2 + x + 1$, i.e. a primitive element of $\mathbb{F}_{2^2} \cong \mathbb{F}_2[\alpha]$. The respective companion matrix is

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Then $\mathcal{G}_{2^2}(1, 2) = \{\text{rs}(1, 0), \text{rs}(1, \alpha), \text{rs}(1, \alpha^2), \text{rs}(1, 1), \text{rs}(0, 1)\}$ and substituting all elements of $\mathbb{F}_{2^2} \cong \mathbb{F}_2[\alpha]$ with its corresponding element from $\mathbb{F}_2[P]$ gives a spread in $\mathcal{G}_2(2, 4)$.

Orbit codes [23] in $\mathcal{G}_q(k, n)$ are defined to be orbits of a subgroup of the general linear group GL_n of order n over \mathbb{F}_q . They can be seen as the analogs of linear codes in classical block coding and their structure can be used for an easy computation of the minimum distance of a code and for decoding algorithms (e.g. one can define coset leader decoding for them). For more information on orbit codes the interested reader is referred to [14], [17], [20], [22]. One can also use the orbit code construction to construct spread codes. Note that this construction of spread codes is not equivalent to the Desarguesian construction from before.

Example 2. The following orbit code is also a spread code in $\mathcal{G}_2(2, 4)$:

$$\text{rs} \left(\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \right) \left\langle \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \right\rangle$$

In general, for any given code \mathcal{C} in some space X and some message space \mathcal{M} , the corresponding encoding map

$$\text{enc} : \mathcal{M} \longrightarrow X$$

is an injective map, mapping any message to a codeword. I.e. $\text{enc}(\mathcal{M}) = \mathcal{C}$. Mostly in the information theory literature $\mathcal{M} = \{0, \dots, j-1\}$ for some integer j . For classical linear block codes the usual message space is $\mathcal{M} = \mathbb{F}_q^k$ for some integer k . If $q = p^r$ for some prime number p , then $\mathbb{F}_q^k \cong \mathbb{F}_p^{rk}$ and the *p-adic expansion*

$$\begin{aligned} \phi : \mathbb{F}_p^{rk} &\longrightarrow \{0, \dots, rk-1\} \\ (u_0, \dots, u_{rk-1}) &\longmapsto x = \sum_{i=0}^{rk-1} u_i p^i \end{aligned}$$

is a bijection. Moreover, ϕ and ϕ^{-1} can be computed very efficiently (for the inverse one recursively computes $u_{i+1} \equiv (x - u_i)/p \pmod p$ with the initial congruence $u_0 \equiv x \pmod p$).

In the subspace coding case it is not obvious what \mathcal{M} would be and how message encoding or decoding can be done. An elegant solution is given for the Reed-Solomon-like codes in [11]. For such a code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ the message space is

$$\mathcal{M} = \mathbb{F}_{q^{n-k}}^{k - \frac{d_S(\mathcal{C})}{2} + 1},$$

which is isomorphic (as a vector space) to $\mathbb{F}_q^{(n-k)(k - \frac{d_S(\mathcal{C})}{2} + 1)}$, and the encoding map is given by

$$\begin{aligned} \text{enc} : \mathbb{F}_{q^{n-k}}^{k - \frac{d_S(\mathcal{C})}{2} + 1} &\longrightarrow \mathcal{G}_q(k, n) \\ (v_0, \dots, v_{k - \frac{d_S(\mathcal{C})}{2} - 1}) &\longmapsto \langle (\beta_j, \sum_{i=0}^{k - \frac{d_S(\mathcal{C})}{2} - 1} v_i \beta_j^i) \mid j = 1, \dots, k \rangle \end{aligned}$$

where β_1, \dots, β_k is a basis of \mathbb{F}_{q^k} over \mathbb{F}_q and we use $\mathbb{F}_q^n \cong \mathbb{F}_{q^n}$ on the right side. Via interpolation this map is invertible and the inverse is computable in polynomial time. Hence, one gets a feasible message decoding map as well.

In the following sections we want to investigate if one can find message encoding maps from a set of integers to orbit and spread codes, whose inverse is efficiently computable, as well.

III. MESSAGE ENCODING FOR DESARGUESIAN SPREAD CODES

We call a spread in $\mathcal{G}_q(k, n)$ Desarguesian if it is isomorphic to $\mathcal{G}_{q^k}(1, m)$ (where $m = n/k$). For simplicity though, we will work only with codes arising from the construction as described in the previous section. Analog results for the equivalent codes can then easily be derived.

Because of the isomorphic description of the code as all elements of $\mathcal{G}_{q^k}(1, m)$, the easiest choice of message space is exactly $\mathcal{M} = \mathcal{G}_{q^k}(1, m)$ and the encoding map is the second point of the construction in Section II. Let α be a primitive element of \mathbb{F}_{q^k} , $p_\alpha(x) \in \mathbb{F}_q[x]$ its minimal polynomial and $P_\alpha \in \text{GL}_k$ the corresponding companion matrix. Then $\mathbb{F}_{q^k} \cong \mathbb{F}_q[\alpha]$ and any element in \mathbb{F}_{q^k} can be expressed as a polynomial in α of degree less than k , and one can define the following encoding map:

$$\begin{aligned} \text{enc}_1 : \mathcal{G}_{q^k}(1, m) &\longrightarrow \mathcal{G}_q(k, n) \\ \text{rs} \left(\sum_{i=0}^{k-1} u_{1i} \alpha^i, \dots, \sum_{i=0}^{k-1} u_{mi} \alpha^i \right) &\longmapsto \text{rs} \left(\sum_{i=0}^{k-1} u_{1i} P^i, \dots, \sum_{i=0}^{k-1} u_{mi} P^i \right). \end{aligned}$$

This map is well defined, since all non-zero elements of $\mathbb{F}_q[P]$ have full rank and hence the right side is always an element of $\mathcal{G}_q(k, n)$. Note that the left side is represented by a basis vector over \mathbb{F}_{q^k} , whereas the right side is represented by a matrix in $\mathbb{F}_q^{k \times n}$, whose row space is the corresponding codeword.

Theorem 3. *The map enc_1 is injective.*

Proof: This follows from the isomorphism $\mathbb{F}_q[\alpha] \cong \mathbb{F}_q[P]$, since $f(\alpha) = g(\alpha)$ if and only if $f(P) = g(P)$ for any $f(x), g(x) \in \mathbb{F}_q[x]$. ■

Thus, one can derive an inverse map, called the decoding map. In this case the decoding map is again very simple, and since none of the codewords intersect in a non-zero element, it is enough to consider only one non-zero vector $v \in \mathbb{F}_q^n$ of the codeword to recover the message. For this we translate that vector v into a vector over \mathbb{F}_{q^k} , i.e. we partition v into blocks of length k and represent these blocks in their extension field representation ($\mathbb{F}_q^k \cong \mathbb{F}_{q^k} \cong \mathbb{F}_q[\alpha]$). This is then a basis of the corresponding message in $\mathcal{G}_{q^k}(1, m)$.

If one wants to have a unique description of the messages, one can choose the normalized basis vector, i.e. the one element of the one-dimensional subspace whose first non-zero entry is equal to one. In the message decoding process, one needs to add an additional step then, that divides all elements of the vector in $\mathbb{F}_{q^k}^m$ by the first non-zero entry of that new vector.

The reader familiar with projective spaces will notice that $\mathcal{G}_{q^k}(1, m)$ corresponds exactly to the projective space over \mathbb{F}_{q^k} of dimension $m-1$. The usage of a normalized representative of points in that space is a common concept there.

Theorem 4. For a code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ the decoding map $\text{enc}_1^{-1} : \mathcal{C} \rightarrow \mathcal{G}_{q^k}(1, m)$ can be computed with a complexity of order $\mathcal{O}_q(kn)$.

Proof: Choose one vector $v \in \mathbb{F}_q^n$ of the given codeword and represent it as an element of $\mathbb{F}_{q^k}^m$. For the normalization, one needs at most $m = n/k$ divisions over \mathbb{F}_{q^k} . Each such division can be done with $\mathcal{O}_q(k^2)$ operations. ■

Note, that in the spread decoding algorithm of [13] one gets the normalized representation of the message along the way in the algorithm and the additional step of message decoding is not necessary.

In the following we will show how one can also encode the message set $\mathcal{M} = \{1, \dots, (q^n - 1)/(q^k - 1)\}$ by concatenating enc_1 with yet another map:

$$f : \{1, \dots, (q^n - 1)/(q^k - 1)\} \rightarrow \mathcal{G}_{q^k}(1, m)$$

$$i \mapsto \langle \underbrace{(0, \dots, 0)}_{\epsilon(i)}, 1, \phi_i^{-1}(i - \sum_{j=0}^{\epsilon(i)-1} q^{jk}) \rangle.$$

where $\epsilon(i) := m - \min\{y \mid \sum_{j=0}^{y-1} q^{jk} \geq i\}$ and $\phi_i : \mathbb{F}_{q^k}^{m-\epsilon(i)-1} \rightarrow \{1, \dots, q^{k(m-\epsilon(i)-1)}\}$ is the p -adic expansion, as explained in Section II.

Theorem 5. The map f is bijective and hence

$$\text{enc}_2 := \text{enc}_1 \circ f$$

is an injective map from $\{1, \dots, (q^n - 1)/(q^k - 1)\}$ to $\mathcal{G}_q(k, n)$.

Proof: We show that f is injective, then by the equal cardinalities of domain and codomain it is automatically bijective. It holds that 1 is mapped to $\langle (0, \dots, 0, 1) \rangle$, $\{2, \dots, q^k + 1\}$ is mapped to $\langle (0, \dots, 0, 1, \mathbb{F}_{q^k}) \rangle$, $\{q^k + 2, \dots, q^{2k} + q^k + 1\}$ is mapped to $\langle (0, \dots, 0, 1, \mathbb{F}_{q^k}^2) \rangle$, etc. Since ϕ_i is bijective, the statement follows. ■

As before, one can easily find the inverse map of enc_2 and get a message decoding map for the integer message set as well.

Theorem 6. The maps enc_2 and enc_2^{-1} are computable with a computational complexity of order at most $\mathcal{O}_q(kn)$.

Proof: Since $\epsilon(i)$ only takes $m - 1$ values, one can store these in a look-up table and use an ordered search to find the right value. (But also computing $\epsilon(i)$ without a table can be done efficiently.) Since ϕ_i and ϕ_i^{-1} are efficiently computable, the overall complexity of the inverse map is dominated by the normalization (see Theorem 4). Since the complexity of enc_2 is lower than the one of enc_2^{-1} , the statement follows. ■

Note that due to simplicity we chose $\mathcal{M} = \{1, \dots, (q^n - 1)/(q^k - 1)\}$, but clearly one can change f and thus enc_2 to encode the message set $\{0, \dots, (q^n - 1)/(q^k - 1) - 1\}$.

IV. MESSAGE ENCODING FOR CYCLIC ORBIT CODES

Recall that an orbit code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ is defined as the orbit of a given $\mathcal{U} \in \mathcal{G}_q(k, n)$ under the action of a subgroup G of GL_n . In general it holds that $|\mathcal{C}| \leq |G|$, i.e. some elements of G might generate the same codewords. Denote by

$$\text{stab}_{\text{GL}_n}(\mathcal{U}) := \{A \in \text{GL}_n \mid \mathcal{U}A = \mathcal{U}\}$$

the stabilizer of \mathcal{U} in GL_n , and by $G/\text{stab}_{\text{GL}_n}(\mathcal{U})$ the set of all right cosets $\text{stab}_{\text{GL}_n}(\mathcal{U})A$ for $A \in \text{GL}_n$. Then the encoding map can be defined as

$$\begin{aligned} \text{enc}_3 : G/\text{stab}_{\text{GL}_n}(\mathcal{U}) &\rightarrow \mathcal{G}_q(k, n) \\ [A] &\mapsto \mathcal{U}A. \end{aligned}$$

where $[A]$ denotes the coset of A .

Theorem 7. The map enc_3 is injective.

Proof: Let $A, B \in G$. Assume that $\mathcal{U}A = \mathcal{U}B$, then

$$AB^{-1} \in \text{stab}_{\text{GL}_n}(\mathcal{U})$$

and thus $A = AB^{-1}B \in \text{stab}_{\text{GL}_n}(\mathcal{U})B$. Hence, A and B are in the same right cosets of $\text{stab}_{\text{GL}_n}(\mathcal{U})$. ■

We now want to find an encoding map for orbit codes with respect to the integer numbers as messages. To do so we will restrict ourselves to cyclic orbit codes in this paper, since these have more useful structure. Moreover, cyclic orbit codes are also better understood from a construction and error decoding point of view.

Cyclic orbit codes are those codes that can be defined by the action of a cyclic subgroup G , i.e. $G = \langle P \rangle$ for some matrix $P \in \text{GL}_n$. Then one clearly has a bijection from $\mathcal{M} = \{0, \dots, \text{ord}(P) - 1\}$ to G :

$$\begin{aligned} g' : \{0, \dots, \text{ord}(P) - 1\} &\rightarrow G \\ i &\mapsto P^i. \end{aligned}$$

From group theory (see e.g. [9]) one knows that $|G/\text{stab}_{\text{GL}_n}(\mathcal{U})|$ is a divisor of $|G| = \text{ord}(P)$ and that if $\text{ord}_{\mathcal{U}}(P) := |G/\text{stab}_{\text{GL}_n}(\mathcal{U})| < |G|$, then $\mathcal{U}P^i = \mathcal{U}P^{i+\text{ord}_{\mathcal{U}}(P)}$. Thus it follows:

Lemma 8. The map

$$\begin{aligned} g : \{0, \dots, \text{ord}_{\mathcal{U}}(P) - 1\} &\rightarrow G/\text{stab}_{\text{GL}_n}(\mathcal{U}) \\ i &\mapsto P^i. \end{aligned}$$

is a bijection for any $\mathcal{U} \in \mathcal{G}_q(k, n)$.

Corollary 9. The map $\text{enc}_4 := \text{enc}_3 \circ g$ is injective and hence an encoding map for the message set $\mathcal{M} = \{0, \dots, \text{ord}_{\mathcal{U}}(P) - 1\}$.

Note that enc_4 can be computed very efficiently while its inverse is a discrete logarithm problem (DLP), which is in general a hard problem. There are many results on when the DLP is hard and when it is not; for a survey of various algorithms and their complexities see e.g. [16]. In the following we will investigate some of the easy cases, since these will be the one of interest from an application point of view.

A. Primitive Cyclic Orbit Codes

For this subsection let α be a primitive element of \mathbb{F}_{q^n} , $p_\alpha(x) \in \mathbb{F}_q[x]$ its minimal polynomial and P_α the corresponding companion matrix. Denote by $G = \langle P_\alpha \rangle$ the group generated by it. Because of the primitivity it holds that

$$\text{ord}(\alpha) = \text{ord}(P_\alpha) = |G| = q^n - 1.$$

n	$\max p_i$	$\max e_i$	$\max(e_i n, e_i p_i)$	n^2
6	7	3	18	36
8	17	1	17	64
9	73	1	73	81
10	31	1	31	100
11	89	1	89	121
12	13	2	24	144
14	127	1	127	196
15	151	1	151	225
18	73	3	73	324
20	41	2	41	400
21	337	2	337	441
24	241	2	241	576
28	127	1	127	784
30	331	2	331	900
36	109	3	109	1296
48	673	2	673	2304
60	1321	2	1321	3600

TABLE I
 n^2 -SMOOTH $2^n - 1 = \prod_{i=1}^r p_i^{e_i}$.

We call $\mathcal{C} = \mathcal{U}G$ a primitive cyclic orbit code for any $\mathcal{U} \in \mathcal{G}_q(k, n)$. For more information on the cardinality and minimum distance of different primitive cyclic orbit codes the interested reader is referred to [22], but we want to remark that for any valid set of parameters one can construct a spread code as a primitive cyclic orbit code. In this case one constructs \mathcal{U} in such a way that $q^k - 1$ of its non-zero elements are in its own stabilizer $\text{stab}_{\text{GL}_n}(\mathcal{U})$ and hence $G/\text{stab}_{\text{GL}_n}(\mathcal{U}) = (q^n - 1)/(q^k - 1)$.

Using the Pohlig-Hellman algorithm for DLP [15, Sec. 3.6.3], one can compute a solution for the discrete logarithm with a computational complexity of order $\mathcal{O}_{q^n}(\sum_{i=1}^r e_i(\log_2 q^n + \sqrt{p_i})) \leq \mathcal{O}_q(n^2 \sum_{i=1}^r e_i(\log_2 q^n + \sqrt{p_i}))$ where $\prod_{i=1}^r p_i^{e_i}$ is the prime factorization of $q^n - 1$.

For simplicity we will now concentrate on the case $q = 2$. If $q = 2$, the above complexity becomes

$$\mathcal{O}_2(n^2 \sum_{i=1}^r e_i(n + \sqrt{p_i})).$$

Hence, if $2^n - 1$ is n^2 -smooth (i.e. if all prime factors of $2^n - 1$ are less than or equal to n^2) and the largest e_i is less than or equal to k , then the order of this complexity is upper bounded by $\mathcal{O}_2(n^3 k)$, which is reasonable. For this note e.g. that the complexities of the decoders in [11], [18] are at least cubic in n . The decoding complexities of the two error decoding algorithms for primitive cyclic orbit codes in [22] are of order $\mathcal{O}_2(4^k(n^2 + k^2 n))$ and $\mathcal{O}_2(nk(nk - k^2 - n))$, respectively. Thus, in most cases, the message decoding would not drastically increase the overall complexity.

Table I shows values of n for which $2^n - 1$ is n^2 -smooth. As one can see, also the largest exponent e_i is small, hence the above statement holds for many values of k .

Thus, we have shown that there exist parameters for which enc_4 is a message encoding function for orbit codes, that has an efficient inverse map, i.e. an efficient corresponding decoder. For many parameters though, the procedures described in this section are not efficiently computable, which is why

we derive other algorithms for the special class of orbit spread codes in the next section.

V. A HYBRID EN- AND DECODER FOR SPREAD CODES

As mentioned in the previous section, orbit codes have useful structure, which can be exploited for error decoding. E.g. the coset leader decoding algorithm for irreducible cyclic orbit codes from [22] has a very low computational complexity. Spread codes are among the most interesting constant dimension codes because of their optimal tradeoff between error correction capability and transmission rate. As mentioned before, they can be constructed as primitive cyclic orbit codes, and we can hence use the coset leader decoder for them. On the other hand, we have an efficient message en- and decoder for Desarguesian spreads, as described in Section III. In this section we want to combine the message en- and decoder for Desarguesian spread codes with the error correction en- and decoder for orbit codes, which we call a *hybrid en- and decoder* for spread codes.

For this assume that there exist a Desarguesian spread code $S_1 \in \mathcal{G}_q(k, n)$ and a primitive cyclic orbit spread code $S_2 \in \mathcal{G}_q(k, n)$, such that $S_1 A = S_2$ (as sets of vector spaces) for some $A \in \text{GL}_n$. Then we can define the following encoding map for the message space $\mathcal{M} = \{1, \dots, (q^n - 1)(q^k - 1)\}$:

$$\begin{aligned} \text{enc}_5 : \quad \mathcal{M} &\longrightarrow \mathcal{G}_q(k, n) \\ i &\longmapsto \text{enc}_2(i)A \end{aligned}$$

Theorem 10. *The map enc_5 is injective and both enc_5 and enc_5^{-1} are computable with a computational complexity of order at most $\mathcal{O}_q(kn^2)$.*

Proof: The multiplication with A can be done with the order of $\mathcal{O}_q(kn^2)$, which dominates the complexity order of enc_2 . The inverse A^{-1} can be precomputed and stored and hence in the decoding map the multiplication with A^{-1} has the same complexity, or only $\mathcal{O}_q(n^2)$, if we use only one vector as representative of the whole vector space. The same computations can naturally also be done in the extension field representation, using $\mathbb{F}_q^n \cong \mathbb{F}_{q^n}$. ■

Moreover, $\text{enc}_5(\mathcal{M}) = S_2$, i.e. we send codewords of S_2 over the channel and can use the corresponding error decoding algorithms for cyclic orbit codes, before we then apply enc_5^{-1} to recover the message. Note that this gives an efficient message en- and decoder for primitive cyclic orbit spread codes, independent of the discrete logarithm problem.

It remains to show that there are Desarguesian spread codes that are related to primitive cyclic orbit codes by a linear transformation. In this case one also says that they are linearly isometric (see [20], [21]). It was shown in [21] that not all spreads are linearly isometric, i.e. you cannot always find a linear map from one spread in $\mathcal{G}_q(k, n)$ to another spread in $\mathcal{G}_q(k, n)$. On the other hand, it was also shown that all Desarguesian spreads are linearly isometric. Hence, for our purposes, it remains to investigate when a primitive cyclic orbit spread code is a Desarguesian spread. This can be done by using the algorithm of [5], or by using the following results: Desarguesian spreads are always orbit codes [23], and

two orbit codes are linearly isometric if and only if their generating groups are conjugates [14]. Furthermore, if one of two conjugate groups is cyclic, also the other one is cyclic and there exist two respective generator matrices of the two groups, that are similar. This way, one can check if a given Desarguesian spread code is linearly isometric to a given cyclic orbit spread code. We will illustrate one such pair of codes in the following and concluding example.

Example 11. Let S_1 be the spread constructed in Example 1 and let S_2 be the orbit spread code constructed in Example 2, both subsets of $\mathcal{G}_2(2, 4)$. Then

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

is a linear transformation from S_1 to S_2 . Let β be a primitive element of \mathbb{F}_{q^n} . In the isomorphic extension field representation, A maps the basis $\{1, \beta, \beta^2, \beta^3\}$ of \mathbb{F}_{q^n} over \mathbb{F}_q to the new basis $\{1, \beta + \beta^2, 1 + \beta, \beta + \beta^3\}$. We can now use S_1 for message encoding, say we got the codeword $c \in S_1$, then we send the codeword $cA \in S_2$ over the channel. We can then do error correction decoding in the code S_2 with any orbit decoder (e.g. with coset leader decoding), say we get the codeword $c' \in S_2$, and transform it to $c'A^{-1} \in S_1$, from which we can then easily get the message as explained in Section III.

VI. CONCLUSION

In this work we investigate how message encoding can be done for spread and orbit codes, two families of subspace codes that have been well studied for error correction in random network coding.

We show that for Desarguesian spread codes one can find encoding maps such that the map itself and the inverse map are efficiently computable. We also show that for general cyclic orbit codes message decoding translates to a discrete logarithm problem, which is efficiently computable for some sets of parameters, but not in general. In the end we propose a hybrid en- and decoder for spread codes, such that one can use the orbit structure for error correction, but avoid the discrete logarithm problem in the message decoding part.

The results for orbit codes are shown for primitive cyclic orbit codes, but a generalization to arbitrary irreducible cyclic orbit codes is straight-forward. Furthermore, with some more effort one can then generalize these results to general cyclic orbit codes.

An open question for further research is if one can find general results on when cyclic orbit spread codes are Desarguesian and how to find the linear transformation from one spread into the other without the help of the algorithm of [5]. Moreover, one can investigate if there are other codes where a hybrid en- and decoder can be helpful to combine efficient error correction decoders with efficient message decoders.

REFERENCES

- [1] M. Bossert and E.M. Gabidulin. One family of algebraic codes for network coding. In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pages 2863–2866, 2009.
- [2] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Transactions on Information Theory*, 55(7):2909–2919, March 2009.
- [3] T. Etzion and N. Silberstein. Codes and designs related to lifted MRD codes. *IEEE Transactions on Information Theory*, 59(2):1004–1017, 2013.
- [4] T. Etzion and A. Vardy. Error-correcting codes in projective space. *IEEE Transactions on Information Theory*, 57(2):1165–1173, 2011.
- [5] T. Feulner. Canonical forms and automorphisms in the projective space. *preprint*, 2012.
- [6] E. M. Gabidulin and N. I. Pilipchuk. Multicomponent network coding. In *Proceedings of the Seventh International Workshop on Coding and Cryptography (WCC) 2011*, pages 443–452, Paris, France, 2011.
- [7] M. Gadouleau and Z. Yan. Constant-rank codes and their connection to constant-dimension codes. *IEEE Transactions on Information Theory*, 56(7):3207–3216, 2010.
- [8] E. Gorla, F. Manganiello, and J. Rosenthal. An algebraic approach for decoding spread codes. *Advances in Mathematics of Communications (AMC)*, 6(4):443–466, 2012.
- [9] A. Kerber. *Applied finite group actions*, volume 19 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, second edition, 1999.
- [10] A. Kohnert and S. Kurz. Construction of large constant dimension codes with a prescribed minimum distance. In J. Calmet, W. Geiselmann, and J. Müller-Quade, editors, *MMICS*, volume 5393 of *Lecture Notes in Computer Science*, pages 31–42. Springer, 2008.
- [11] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.
- [12] F. Manganiello, E. Gorla, and J. Rosenthal. Spread codes and spread decoding in network coding. In *Proceedings of the 2008 IEEE International Symposium on Information Theory*, pages 851–855, Toronto, Canada, 2008.
- [13] F. Manganiello and A.-L. Trautmann. Spread decoding in extension fields. *arXiv:1108.5881v1 [cs.IT]*, to appear in *Finite Fields and Applications*, 2011.
- [14] F. Manganiello, A.-L. Trautmann, and J. Rosenthal. On conjugacy classes of subgroups of the general linear group and cyclic orbit codes. In *Proceedings of the 2011 IEEE International Symposium on Information Theory*, pages 1916–1920, St. Petersburg, Russia, 2011.
- [15] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.
- [16] A.M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *Advances in Cryptology*, volume 209 of *Lecture Notes in Computer Science*, pages 224–314. Springer Berlin Heidelberg, 1985.
- [17] J. Rosenthal and A.-L. Trautmann. A complete characterization of irreducible cyclic orbit codes and their Plücker embedding. *Designs, Codes and Cryptography*, 66:275–289, 2013.
- [18] D. Silva, F. R. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, 2008.
- [19] V. Skachek. Recursive code construction for random networks. *Information Theory, IEEE Transactions on*, 56(3):1378–1382, 2010.
- [20] A.-L. Trautmann. *Constructions, Decoding and Automorphisms of Subspace Codes*. PhD thesis, University of Zurich, Switzerland, 2013.
- [21] A.-L. Trautmann. Isometry and automorphisms of constant dimension codes. *Advances in Mathematics of Communications (AMC)*, 7(2):147–160, 2013.
- [22] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal. Cyclic orbit codes. *IEEE Transactions on Information Theory*, 59(11):7386–7404, 2013.
- [23] A.-L. Trautmann, F. Manganiello, and J. Rosenthal. Orbit codes - a new concept in the area of network coding. In *IEEE Information Theory Workshop (ITW)*, pages 1–4, Dublin, Ireland, 2010.
- [24] A.-L. Trautmann and J. Rosenthal. New improvements on the echelon-Ferrers construction. In *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS*, pages 405–408, Budapest, Hungary, 2010.